ACTA ARITHMETICA
LXXX.4 (1997)

Upper bounds for least witnesses and generating sets

by

Ronald Joseph Burthe Jr. (Columbia, Md.)

1. Introduction to $G(n)$ and $w(n)$. For $n, y \in \mathbb{Z}^+$, let $\mathcal{G}_n(y)$ denote the subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ generated by the elements of $(\mathbb{Z}/n\mathbb{Z})^*$ with representatives not exceeding y. Define $G(n)$ to be the smallest G such that $\mathcal{G}_n(G) = (\mathbb{Z}/n\mathbb{Z})^*$.

For those positive integers n which have primitive roots, an upper bound for its first primitive root is also an upper bound for $G(n)$. For those n without primitive roots, the minimal number of elements needed to generate $(\mathbb{Z}/n\mathbb{Z})^*$ will not exceed $G(n) - 1$.

If n has r distinct prime factors we see from the Chinese Remainder Theorem that $(\mathbb{Z}/n\mathbb{Z})^*$ requires $r-1$, r, or $r+1$ generators depending upon the power of 2 dividing n (i.e. $r-1$ if $2 \parallel n$, r if $2 \nmid n$ or $4 \parallel n$, and $r+1$ otherwise). If $(\mathbb{Z}/n\mathbb{Z})^*$ has g generators, then $G(n)$ must be greater than or equal to the gth prime which does not divide n. Thus we must have $G(n) \geq p_r$ where p_r is the rth prime. By the prime number theorem $p_r \sim r \log r$ as $r \to \infty$ and since the normal order of the number of distinct prime factors of n is $\log\log n$ (see [HW]), for every $\varepsilon > 0$ we have $G(n) > (1-\varepsilon)\log\log n \log\log\log n$ for a set of integers n with asymptotic density 1.

In 1949, Fridlender [F] and Salié [S] proved independently that for prime p the first quadratic non-residue mod p is $\Omega(\log p)$; that is, there is a positive constant c such that the first quadratic non-residue mod p is greater than $c \log p$ for infinitely many primes p. Since the quadratic residues mod p cannot generate $(\mathbb{Z}/p\mathbb{Z})^*$, $G(p)$ must be at least as large as the first quadratic non-residue mod p. Thus, $G(p) = \Omega(\log p)$. Graham and Ringrose [GR] improved this result by showing that the first quadratic non-residue modulo a prime p is $\Omega(\log p \log\log\log p)$. Thus, $G(p) = \Omega(\log p \log\log\log p)$.

Granville has made the observation that from the Graham–Ringrose result one can conclude that for every $\varepsilon > 0$ there is a positive constant k_ε and infinitely many integers x such that the number of integers $n \leq x$ with

1991 *Mathematics Subject Classification*: Primary 11A51.

$G(n) > k_\varepsilon \log n \log\log\log n$ is at least $x^{1-\varepsilon}$. To see this, note that if p is a prime dividing n, then $G(p) \le G(n)$. This inequality follows from the fact that a set of generators for $(\mathbb{Z}/n\mathbb{Z})^*$ must also be a set of generators for $(\mathbb{Z}/p\mathbb{Z})^*$. Now let c be the constant from the Graham–Ringrose result and let p be a prime such that $G(p) \ge c \log p \log\log\log p$. Taking $x = \lceil p^{1/\varepsilon} \rceil$, choosing $n \le x$ such that $p \mid n$, and using the above inequality we see for x sufficiently large that

$$\begin{aligned} G(n) &\ge c \log p \log\log\log p > (c\varepsilon/2) \log x \log\log\log x \\ &\ge (c\varepsilon/2) \log n \log\log\log n. \end{aligned}$$

Since the number of multiples of p less than or equal to x is about $x/p \ge x/x^\varepsilon = x^{1-\varepsilon}$, we thus get the result.

A result from Burgess [Bu1] implies that for all primes p, $G(p) = O_\varepsilon(p^{1/4+\varepsilon})$. Following the work of Ankeny in [A], Montgomery showed in [Mo] that the Generalized Riemann Hypothesis (GRH) implies that $G(n) = O(\log^2 n)$. In 1990 in [B2], Bach showed, assuming the GRH, that one could take 3 as the implied constant and verified that $G(n) \le 3 \log^2 n$ for all positive integers $n \le 10^6$.

In 1993 Konyagin–Pomerance [KP] and Pappalardi [Pa] independently proved that for all $\varepsilon > 0$ and for all primes $p \le x$, $G(p) \le x^\varepsilon$ with at most $O_\varepsilon(1)$ exceptions.

Bach and Huelsbergen conjecture in [BH] that

$$G(n) \le [(\log 2)^{-1} + o(1)] \log n \log\log n$$

as $n \to \infty$ and that the constant $(\log 2)^{-1}$ is the best possible. They prove (via the Pólya–Vinogradov inequality) that

$$G(n) = O(\sqrt{n} \log n \log\log n).$$

In this paper we will prove that for all positive integers n, $G(n) = O_\varepsilon(n^{1/(3\sqrt{e})+\varepsilon})$, and for $8 \nmid n$, $G(n) = O_\varepsilon(n^{1/(4\sqrt{e})+\varepsilon})$. The exponent for the general upper bound was $3/(8\sqrt{e})$ in my dissertation but as suggested by Karl Norton one can replace it with a $1/(3\sqrt{e})$ by using a more recent result of Burgess. It should also be noted that Karl Norton has communicated to me via a personal correspondence that he has advanced some of the ideas in this paper and can show that $G(n) = O_\varepsilon(n^{1/(4\sqrt{e})+\varepsilon})$ for *all* positive integers n.

We now show a connection between $G(n)$ and primality tests.

Let n be a positive odd number greater than 1 with $n - 1 = 2^s t$ where t is odd. For $a \in [1, n-1]$, we say that n is a *strong pseudoprime to base* a if

(1) *either* $a^t \equiv 1 \bmod n$ *or*

$$a^{2^i t} \equiv -1 \bmod n \quad \text{for some } i \in \{0, 1, \ldots, s-1\}.$$

If n is an odd prime then (1) holds for all $a \in [1, n-1]$. If (1) fails for some $a \in [1, n-1]$, then a is called a *witness* (to the compositeness) of n.

In the 70s, Selfridge was able to identify composite numbers fairly quickly using (1), which has the advantage over other similar pseudoprimality tests in that there are no odd composites n which will satisfy (1) for all a in $[1, n-1]$ that are coprime to n. It was shown independently by Monier [M] and Rabin [R] that for each odd composite n at least three fourths of the integers a in $[1, n-1]$ will be witnesses for n. This method leads to a probabilistic algorithm that can determine the compositeness of an integer but cannot prove primality.

To develop an algorithm which could prove primality, it would suffice to find a finite set of "reliable witnesses" such that every odd composite n has a witness in this set. Erdős [E] and Pomerance [P1] have shown that any fixed integer is a witness for most odd composite n so it might seem possible to construct such a set. However, Alford, Granville, and Pomerance have shown in [AGP] that for any finite set of integers, there are infinitely many odd composite integers which have no witnesses in that set.

It is then natural to ask what can be said about the least positive witness, denoted by $w(n)$, for an odd composite n. From the results previously stated, $w(n)$ will be 2 for most n, but can get arbitrarily large. Since every composite n has a prime divisor not exceeding $\sqrt{n}$, a trivial upper bound for $w(n)$ is $\sqrt{n}$. However, the works of Ankeny, Weinberger, Oesterlé, and Bach (see [B1]) show that if the Generalized Riemann Hypothesis (GRH) holds, then $w(n) < 2\log^2 n$ for all odd composite n. Thus, if the GRH holds we would have a polynomial time deterministic primality test.

In this paper, we prove that for all $\varepsilon > 0$, $w(n) = O_\varepsilon(n^{(6\sqrt{e})^{-1}+\varepsilon})$ for all odd composite n.

It should also be noted that a heuristic argument of the type done by Bach and Huelsbergen indicates that $w(n) \le ((\log 4)^{-1} + o(1)) \log n \log\log n$ as $n \to \infty$ through the odd composites and the constant $(\log 4)^{-1}$ is optimal.

Also, Alford, Granville, and Pomerance showed in [AGP] by assuming a version of the prime k-tuplets conjecture that the maximal order of $w(n)$ exceeds $\alpha \log n$ for some $\alpha > 0$. They also give a heuristic argument that the maximal order of $w(n)$ should be $c \log n \log\log n$ for some constant $c > 0$. They prove that $w(n) > (\log n)^{1/(3\log\log\log n)}$ infinitely often.

I would like to thank Carl Pomerance for his extensive help in the writing of this paper. I would also like to thank Karl Norton for his insights and simplifications in regards to this paper and for providing me with several related references.

2. Preliminaries. In this section various results concerning $G(n)$ and $w(n)$ are proved, including connections with Dirichlet characters mod n.

The following results will be especially helpful in proving our main theorem. For a non-principal Dirichlet character χ, let $B(\chi)$ denote the least positive integer a such that $\chi(a) \neq 1$ and $\chi(a) \neq 0$. Also, χ_0 will always denote the principal character mod n. We take $B(\chi_0) = 0$.

PROPOSITION 2.1. *For all positive integers n,*

$$G(n) = \max_{\chi \bmod n} \{B(\chi)\}.$$

Proof. Let H denote the proper subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ generated by the positive integers that are coprime to n and strictly less than $G(n)$. Since every finite abelian group is a direct product of cyclic groups of prime power order, we can write

$$(\mathbb{Z}/n\mathbb{Z})^*/H \cong \langle\zeta_1\rangle \times \ldots \times \langle\zeta_l\rangle$$

where each ζ_i is a $p_i^{a_i}$th root of unity. Using the series of maps

$$(\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*/H \cong \langle\zeta_1\rangle \times \ldots \times \langle\zeta_l\rangle \to \mathbb{C}^* \tag{2}$$

where the first mapping is the quotient map and the last is the projection map to the first coordinate, we can define a homomorphism $\chi_n : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ such that $\chi_n(h) = 1$ for every $h \in H$. We can extend χ_n to $\mathbb{Z}/n\mathbb{Z}$ by letting $\chi_n(a) = 0$ for $(a, n) > 1$ and thus make it a Dirichlet character mod n. Also note that χ_n is non-principal as $(\zeta_1, 1, \ldots, 1) \in \langle\zeta_1\rangle \times \ldots \times \langle\zeta_l\rangle$ is not sent to 1 by the projection map in (2). Using the surjectivity of the other two maps, we can find an a in $(\mathbb{Z}/n\mathbb{Z})^*$ such that $\chi_n(a) \neq 1$. Now $\chi_n(b) = 1$ for every $b \in H$ and $\chi_n(b) = 0$ for every b with $1 \leq b < G(n)$ and $(b, n) > 1$. Thus, $B(\chi_n) \geq G(n)$, so that

$$G(n) \leq \max_{\chi \bmod n} \{B(\chi)\}.$$

It remains to prove the reverse inequality. Let χ be a non-principal character mod n. If $B(\chi) > G(n)$, then for all a with $1 \leq a \leq G(n)$ and $(a, n) = 1$ we would have $\chi(a) = 1$. Since by definition of $G(n)$ these a's generate $(\mathbb{Z}/n\mathbb{Z})^*$, we would then have $\chi(b) = 1$ for all $b \in (\mathbb{Z}/n\mathbb{Z})^*$. This implies that $\chi = \chi_0$, which is a contradiction. Thus we must have $B(\chi) \leq G(n)$ for all non-principal characters χ mod n. Since $B(\chi_0) = 0$, this inequality holds for all χ mod n and this concludes our proof.

As was pointed out by Karl Norton, one can also show the existence of a non-principal character that is the identity on H by applying his Lemma 3.1 of [N2].

For prime p and $a \in \mathbb{Z}^+$ with $p \nmid a$, let $l_a(p)$ denote the order of a mod p (i.e. the smallest positive integer l such that $a^l \equiv 1 \bmod p$). Also for prime r, let $\nu_r(m)$ denote the largest integer ν such that $r^\nu \mid m$.

The following simple lemmas will prove useful.

LEMMA 2.2. *If n is a strong pseudoprime to base a* (see (1)), *and p and q are distinct primes dividing n, then $\nu_2(l_a(p)) = \nu_2(l_a(q))$. Thus, if n is an odd composite divisible by primes p, q and if $a \in [1, n-1]$ with $\nu_2(l_a(p)) \neq \nu_2(l_a(q))$, then a must be a witness for n.*

P r o o f. If n is a strong pseudoprime to base a with $n-1 = 2^s t$ where $2 \nmid t$, then either $a^{2^i t} \equiv -1 \bmod n$ for some i with $0 \leq i \leq s-1$ or $a^t \equiv 1 \bmod n$. In the former case we see that $\nu_2(l_a(p)) = \nu_2(l_a(q)) = i+1$ and in the latter that $\nu_2(l_a(p)) = \nu_2(l_a(q)) = 0$. So if n is a strong pseudoprime to base a, then we must have $\nu_2(l_a(p)) = \nu_2(l_a(q))$.

It should be noted that a stronger result than Lemma 2.2 holds; namely, that an odd composite integer n is a strong pseudoprime to base a if and only if $a^{n-1} \equiv 1 \bmod n$ and for all odd primes p, q dividing n, we have $\nu_2(l_a(p)) = \nu_2(l_a(q))$ (see [PSW] or [AGP]). Lemma 2.2 will, however, suffice for our purposes.

LEMMA 2.3. *If n is odd and p and q are primes dividing n with $\nu_2(p-1) < \nu_2(q-1)$, and if $a \in [1, n-1]$ is such that $(a/q) = -1$, then a is a witness for n. Furthermore, if $\nu_2(p-1) = \nu_2(q-1)$ and $b \in [1, n-1]$ is such that $(b/(pq)) = -1$, then b is a witness for n.*

P r o o f. First assume that $\nu_2(p-1) < \nu_2(q-1)$ and $(a/q) = -1$. Since $(a/q) = -1$, we see by Euler's Criterion that $\nu_2(l_a(q)) = \nu_2(q-1)$. Since $\nu_2(l_a(p)) \leq \nu_2(p-1) < \nu_2(q-1) = \nu_2(l_a(q))$, we must have $\nu_2(l_a(p)) < \nu_2(l_a(q))$ and thus by Lemma 2.2, a is a witness for n.

Now assume that $\nu_2(p-1) = \nu_2(q-1)$ and $(b/(pq)) = -1$. Without loss of generality we can assume that $(b/p) = 1$ and $(b/q) = -1$. Thus by Euler's Criterion $\nu_2(l_b(p)) < \nu_2(p-1) = \nu_2(q-1) = \nu_2(l_b(q))$ and by Lemma 2.2, b must be a witness of n.

This concludes the proof of Lemma 2.3.

LEMMA 2.4. *For all odd composite n, $w(n) \leq G(n)$.*

P r o o f. Using the notation defined in Section 1 let $T = \mathcal{G}_n(w(n)-1)$. To show that $w(n) \leq G(n)$ it will suffice to show that T is proper subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$.

Assume n is a prime power, say $n = p^a$ where $a \geq 2$. Since none of the integers y with $1 \leq y \leq w(n)-1$ are witnesses for n, for each such y, $y^{n-1} \equiv 1 \bmod n$. Let g be a primitive root for n. Since $\phi(n) = p^{a-1}(p-1)$ does not divide $n-1 = p^a - 1$, we have $g^{n-1} \not\equiv 1 \bmod n$. The set $F = \{1 \leq b \leq n : b^{n-1} \equiv 1 \bmod n\}$ is actually a subgroup under multiplication mod n. Since F contains the subgroup T and does not contain g, it must be that F, and so T, are proper subgroups of $(\mathbb{Z}/n\mathbb{Z})^*$ and $w(n) \leq G(n)$ in this case.

Now assume that n is not a prime power. We will prove this case using an argument of Lenstra (see [Len]) which is also mentioned in [P2]. Let p, q be two distinct primes dividing n.

Suppose that $\nu_2(p-1) < \nu_2(q-1)$. Let λ be the character mod n induced by $(/q)$. If $\lambda(b) = -1$, then by Lemma 2.3, b will be a witness for n. So for each y with $1 \le y \le w(n)-1$ we must have $\lambda(y) = 1$ and thus from Proposition 2.1 we see that $w(n) \le B(\lambda) \le G(n)$.

Thus, we may assume that $\nu_2(p-1) = \nu_2(q-1)$. Let λ be the character mod n induced by $(/p)\cdot(/q)$. If $\lambda(b) = -1$, then by Lemma 2.3, b will be a witness of n. So for each y with $1 \le y \le w(n)-1$ we must have $\lambda(y) = 1$ so $w(n) \le B(\lambda) \le G(n)$ by Proposition 2.1.

This concludes our proof.

Lemma 2.5. *For composite n let χ_n be a non-principal character mod n with $G(n) = B(\chi_n)$* (see Proposition 2.1), *and let ψ* mod d *be the primitive character which induces it. Then $w(n) \le B(\psi)$.*

Proof. Let $a = B(\psi)$. If $\chi_n(a) = 1$ then $(a,n) = 1$ and $\psi(a) = \chi_n(a) = 1$, which contradicts the definition of a. Also $\chi_n(a) = 0$ implies that $(a,n) > 1$ and thus a is a witness for n and thus $w(n) \le a$. Lastly, if $\chi_n(a) \notin \{0,1\}$, then $a \ge B(\chi_n) = G(n) \ge w(n)$ by Proposition 2.1 and Lemma 2.4. So in each case we have $w(n) \le B(\psi)$.

3. Upper bounds for $G(n)$. In this section, we prove theorems that give new upper bounds for $G(n)$. The following lemmas will be useful in the proof of these theorems.

Let $\phi(H,n)$ denote the number of integers x with $1 \le x \le H$ that are coprime to n. Also let $\psi(H,y)$ denote the number of integers x with $1 \le x \le H$ that are y-smooth (i.e. have no prime factors exceeding y) and let $\psi_n(H,y)$ denote the number of integers x with $1 \le x \le H$ such that $(x,n) = 1$ and x is y-smooth.

Lemma 3.1. *For $n \in \mathbb{Z}^+$ and $H > 0$,*

$$\phi(H,n) = \frac{\phi(n)}{n}H + O(d(n))$$

where $d(n)$ is the number of positive divisors of n.

Proof. It is straightforward using the inclusion-exclusion principle to show that

$$\phi(H,n) = \sum_{d|n} \mu(d)\lfloor H/d \rfloor$$

where $\mu(d)$ is the Möbius function. Since $\sum_{d|n}\mu(d)/d = \phi(n)/n$, the result holds.

Approximations for $\psi_n(H,y)$ will be vital in proving our next theorem. Vinogradov [Vi] derived an asymptotic formula for $\psi_n(H,y)$ and stated several inequalities for it which later turned out to be incorrect. Norton uses an asymptotic formula for $\varrho(\alpha)$ (Dickman's function) due to de Bruijn to give a correct version of one of Vinogradov's inequalities. He shows that for $x \geq n$, $x > e^e$, and $e \leq \alpha \leq (\log\log x)/(\log\log\log x)$, there are absolute constants k_1 and k_2 such that

$$\begin{aligned}\psi_n(x, x^{1/\alpha}) &< k_1 \frac{\phi(n)}{n} \varrho(\alpha) x \\ &< k_2 \frac{\phi(n)}{n} x \exp\{-\alpha(\log\alpha + \log\log\alpha - 1 - 1/\log\alpha)\}.\end{aligned}$$

Norton also gives (see Theorems 5.21 and 5.48 in [N1]) more complex estimates for $\psi_n(H,y)$ which are explicitly dependent upon Dickman's function. Fouvry and Tenenbaum showed in [FT] that for every $\varepsilon > 0$, if $\exp\{(\log\log H)^{5/3+\varepsilon}\} \leq y \leq H$, $H \geq H_0(\varepsilon)$, and

$$\log\log(n+2) \leq \left(\frac{\log H}{\log(u+1)}\right)^{1-\varepsilon}$$

where $u = (\log H)/(\log y)$, then

$$\psi_n(H,y) = \psi(H,y)\frac{\phi(n)}{n}\left(1 + O\left(\frac{\log\log(ny)\log\log H}{\log H}\right)\right).$$

For our purposes it will suffice to use the following weaker lemma (see [Bur]).

LEMMA 3.2. *For $n, y \in \mathbb{Z}^+$ and $n^{1/10} \leq H \leq n$, $H^{1/2} \leq y \leq H$, and $H \geq 20$,*

$$\psi_n(H,y) = \frac{\phi(n)}{n} H\left(1 - \log\frac{\log H}{\log y} + O\left(\frac{\log\log\log n}{\log\log n}\right)\right).$$

The following lemmas will give a more general result in Theorem 3.6. Carl Pomerance contributed proofs for Lemmas 3.3 and 3.4 which are used in proving Lemma 3.5 which was suggested by the referee.

For positive integers n, we will say that n is *almost cube-free* if n is cube-free or twice a cube-free number. Recalling the definition of $\nu_r(n)$ preceding Lemma 2.2, n being almost cube-free is also equivalent to having $\nu_r(n) \leq 2$ for every odd prime r and $\nu_2(n) \leq 3$.

LEMMA 3.3. *Let m be a positive integer. Let p be an odd prime such that p^2 divides m. If $\mathcal{S}$ is a set of positive integers which generates $(\mathbb{Z}/m\mathbb{Z})^*$, then $\mathcal{S}$ also generates $(\mathbb{Z}/pm\mathbb{Z})^*$.*

Proof. Let q be a prime such that $q^b \,\|\, m$. Let G_q be the subgroup of $(\mathbb{Z}/m\mathbb{Z})^*$ consisting of those residues that are 1 modulo m/q^b. Then

$G_q \cong (\mathbb{Z}/q^b\mathbb{Z})^*$. Since $\mathcal{S}$ generates $(\mathbb{Z}/m\mathbb{Z})^*$ it will also generate G_q and one may write generators of G_q as words on the elements of $\mathcal{S}$.

Now assume that $p^a \parallel m$ where $a \geq 2$. In this case G_p will be cyclic and thus can be generated by a single word on the elements of $\mathcal{S}$. This word corresponds to a primitive root mod p^a. Since primitive roots mod p^a are also primitive roots mod p^{a+1} for $a \geq 2$, this word in fact corresponds to a primitive root mod p^{a+1}. By the Chinese Remainder Theorem $(\mathbb{Z}/pm\mathbb{Z})^*$ is the direct sum of the various subgroups G_q, so $\mathcal{S}$ must generate the subgroup G_p for $(\mathbb{Z}/pm\mathbb{Z})^*$ as well as the subgroups G_q for $(\mathbb{Z}/pm\mathbb{Z})^*$ for $q \neq p$. Thus $\mathcal{S}$ must generate $(\mathbb{Z}/pm\mathbb{Z})^*$.

LEMMA 3.4. *Let m be a positive integer such that $8 \mid m$. If $\mathcal{S}$ is a set of integers which generate $(\mathbb{Z}/m\mathbb{Z})^*$, then $\mathcal{S}$ will also generate $(\mathbb{Z}/2m\mathbb{Z})^*$.*

Proof. The proof is similar to the previous proof. Although $(\mathbb{Z}/2^a\mathbb{Z})^*$ is not cyclic for $a \geq 3$, it is generated by a pair of elements $\{u, v\}$ in $(\mathbb{Z}/2^a\mathbb{Z})^*$ where none of u, v, uv is 1 mod 8. So in this case if $2^a \parallel m$ and $a \geq 3$, the subgroup G_2 of $(\mathbb{Z}/2^a\mathbb{Z})^*$ will be generated by two words on the elements of $\mathcal{S}$, and the subgroup G_2 of $(\mathbb{Z}/2m\mathbb{Z})^*$ is generated by the same two words. The rest of the proof follows as before.

LEMMA 3.5. *Let d be the largest almost cube-free divisor of a positive integer n. Then $G(d) = G(n)$.*

Proof. If n is almost cube-free then we are done. So assume that n is not almost cube-free.

Let $\mathcal{S}$ be the set of primes less than or equal to $G(d)$ which are coprime to d. So $\mathcal{S}$ generates $(\mathbb{Z}/d\mathbb{Z})^*$. Since n is not almost cube-free, then either $\nu_r(n) \geq 3$ for some odd prime r dividing n or $\nu_2(n) \geq 4$. So either $\nu_r(d) = 2$ or $\nu_2(d) = 3$. In either case, one can apply Lemma 3.3 or Lemma 3.4 by letting $m = d$. By repeated applications of these lemmas, one sees by induction that $\mathcal{S}$ must generate $(\mathbb{Z}/n\mathbb{Z})^*$. Thus $G(d) \geq G(n)$. Since a set of generators for $(\mathbb{Z}/n\mathbb{Z})^*$ will also generate $(\mathbb{Z}/d\mathbb{Z})^*$, we also have $G(d) \leq G(n)$ and thus $G(d) = G(n)$.

THEOREM 3.6. *If χ is a character mod n, then for every $\varepsilon > 0$, we have*

$$B(\chi) = O_\varepsilon(n^{1/(3\sqrt{e})+\varepsilon}).$$

In addition, if $8 \nmid n$, then for all $\varepsilon > 0$,

$$B(\chi) = O_\varepsilon(n^{1/(4\sqrt{e})+\varepsilon}).$$

Proof. From [Bu2] and [Bu3], we know that if χ is a non-principal Dirichlet character mod n, $r \in \mathbb{Z}^+$, n is cube-free or $r = 3$, then for every

$\varepsilon > 0$ and for every pair of integers N, H $(H > 0)$, we have

$$\Big| \sum_{m=N+1}^{N+H} \chi(m) \Big| \ll_{\varepsilon,r} H^{1-1/r} n^{(r+1)/(4r^2)+\varepsilon}.$$

Taking $N = 0$ we see by Burgess' results that

$$\Big| \sum_{m=1}^{H} \chi(m) \Big| \ll_{\varepsilon,r} H^{1-1/r} n^{(r+1)/(4r^2)+\varepsilon} \tag{3}$$

for n cube-free or $r = 3$. We shall take H as a positive integer with $n^{1/10} \le H \le n$ and will specify it more accurately later.

Now define Σ_1 and Σ_2 by

$$\Sigma_1 = \sum_{\substack{m=1 \\ \chi(m)=1}}^{H} 1, \qquad \Sigma_2 = \sum_{\substack{m=1 \\ \chi(m)\notin\{0,1\}}}^{H} 1.$$

Letting $C_{\varepsilon,r}$ denote the constant implicit in (3) and applying the triangle inequality, we see that

$$\begin{aligned} C_{\varepsilon,r} H^{1-1/r} n^{(r+1)/(4r^2)+\varepsilon/2} &\ge \Big| \sum_{m=1}^{H} \chi(m) \Big| = \Big| \sum_{\substack{m=1 \\ \chi(m)=1}}^{H} 1 + \sum_{\substack{m=1 \\ \chi(m)\ne 1}}^{H} \chi(m) \Big| \\ &\ge \sum_{\substack{m=1 \\ \chi(m)=1}}^{H} 1 - \Big| \sum_{\substack{m=1 \\ \chi(m)\ne 1}}^{H} \chi(m) \Big| \\ &\ge \sum_{\substack{m=1 \\ \chi(m)=1}}^{H} 1 - \sum_{\substack{m=1 \\ \chi(m)\notin\{0,1\}}}^{H} 1 = \Sigma_1 - \Sigma_2. \end{aligned}$$

So we have

$$\Sigma_1 - \Sigma_2 \le C_{\varepsilon,r} H^{1-1/r} n^{(r+1)/(4r^2)+\varepsilon}. \tag{4}$$

By definition of Σ_1, Σ_2, and $\phi(H, n)$ (which was defined at the beginning of this section) we also see that

$$\Sigma_1 + \Sigma_2 = \phi(H, n). \tag{5}$$

Let J be a positive number to be identified later. Assume that $J < B(\chi)$. Suppose m is a positive integer counted by $\psi_n(H, J)$; that is, $m \le H$, $(m, n) = 1$, and m is J-smooth. If p is a prime factor of m, then since $(m, n) = 1$, we must also have $(p, n) = 1$ and thus $\chi(p) \ne 0$. And since m is J-smooth, we have $p \le J$. Thus we must have $\chi(p) = 1$ and thus $\chi(m) = 1$. It follows that

$$\Sigma_1 \ge \psi_n(H, J).$$

Applying this inequality and using (4) and (5) we thus see that

$$C_{\varepsilon,r}H^{1-1/r}n^{(r+1)/(4r^2)+\varepsilon} \geq \Sigma_1 - \Sigma_2 = 2\Sigma_1 - (\Sigma_1 + \Sigma_2) \geq 2\psi_n(H,J) - \phi(H,n). \tag{6}$$

Now let $J = H^{1/\sqrt{e}+\delta}$ where δ is a fixed positive constant such that $(\sqrt{e})^{-1} + \delta < 1$. Since $H > J > H^{1/2}$ we see from Lemma 3.2 that there exists a positive constant c such that for n sufficiently large

$$\psi_n(H,J) \geq \frac{\phi(n)}{n} H\left(1 + \log\left(\frac{1}{\sqrt{e}} + \delta\right) - c\frac{\log\log\log n}{\log\log n}\right).$$

Substituting this inequality into (6) and applying Lemma 3.1 we see that

$$\frac{\phi(n)}{n} H\left(1 + 2\log\left(\frac{1}{\sqrt{e}} + \delta\right) - 2c\frac{\log\log\log n}{\log\log n}\right) = O_{\varepsilon,r}(H^{1-1/r}n^{(r+1)/(4r^2)+\varepsilon}) + O(d(n)). \tag{7}$$

By Theorem 328 in [HW] we have $n/\phi(n) = O(\log\log n)$ and from Theorem 315 in [HW] we can take $d(n) = O_\varepsilon(n^\varepsilon)$. Thus, from (7) we have

$$1 + 2\log\left(\frac{1}{\sqrt{e}} + \delta\right) \leq 2c\frac{\log\log\log n}{\log\log n} + O_{\varepsilon,r}(H^{-1/r}n^{(r+1)/(4r^2)+2\varepsilon}) + O_\varepsilon(n^{-\varepsilon}). \tag{8}$$

Note that (8) holds for all $r \in \mathbb{Z}^+$ if n is cube-free and for $r = 3$ for all positive integers n, under the assumption that $J < B(\chi)$.

Now assume that n is cube-free and let $H = \lfloor n^{1/4+1/r} \rfloor$ where $r \in \mathbb{Z}^+$. Thus $H \sim n^{1/4+1/r}$ as $n \to \infty$ and we see that for $\varepsilon = 1/(8r^2)$,

$$H^{-\frac{1}{r}}n^{\frac{r+1}{4r^2}+2\varepsilon} \sim n^{-\frac{1}{4r}-\frac{1}{r^2}+\frac{1}{4r}+\frac{1}{4r^2}+\frac{1}{4r^2}} = n^{-\frac{1}{2r^2}}.$$

Since the exponent is negative, this term goes to 0 as $n \to \infty$. Thus, the right hand side of (8) goes to 0 as $n \to \infty$, which contradicts the fact that $1 + 2\log((\sqrt{e})^{-1} + \delta) > 0$. We conclude that for n sufficiently large

$$B(\chi) \leq J \leq n^{(\frac{1}{4}+\frac{1}{r})(\frac{1}{\sqrt{e}}+\delta)}.$$

Thus, for all $\varepsilon > 0$ and n cube-free,

$$B(\chi) = O_\varepsilon(n^{1/(4\sqrt{e})+\varepsilon}).$$

Now assume that $8 \nmid n$ and let d be the largest almost cube-free divisor of n. Since $8 \nmid n$, d will actually be cube-free and by the result just proved and Proposition 2.1, we see that for all $\varepsilon > 0$,

$$G(d) = O_\varepsilon(d^{1/(4\sqrt{e})+\varepsilon}).$$

From Proposition 2.1 we also see that $B(\chi) \leq G(n)$ and by Lemma 3.5 we have $G(n) = G(d)$. Thus we can conclude that for all $\varepsilon > 0$ and positive

integers n with $8 \nmid n$,

$$B(\chi) = O_\varepsilon(n^{1/(4\sqrt{e})+\varepsilon}).$$

We have actually proved a stronger result; namely, the above equation with n replaced by the largest cube-free divisor of n.

For general n, we take $r = 3$ in (8) and choose $H = \lfloor n^{1/3+9\varepsilon} \rfloor$. Then $H \sim n^{1/3+9\varepsilon}$ as $n \to \infty$, so we see that

$$H^{-1/3} n^{1/9+2\varepsilon} \sim n^{-1/9-3\varepsilon+1/9+2\varepsilon} = n^{-\varepsilon}.$$

Since the exponent is negative we can follow the same argument as before to see that

$$B(\chi) \le J \le n^{(1/3+9\varepsilon)(1/\sqrt{e}+\delta)}.$$

Thus, for every $\varepsilon > 0$, we have

$$B(\chi) = O_\varepsilon(n^{1/(3\sqrt{e})+\varepsilon}).$$

This concludes the proof of Theorem 3.6.

It should be mentioned that the upper bound for $B(\chi)$ for the case where $8 \nmid n$ is not entirely new. Karl Norton has pointed out that one could obtain the same result for cube-free n from a lemma of Kolesnik and Straus (see Lemma 4.8 in [KS]). However, the result for general n appears new.

It should be remarked that Fujii [Fu] proved a result similar to (3) for primitive characters. However, his result includes an involved constant which depends upon the factorization of n and does not in general give an upper bound as small or as clear as Burgess'.

COROLLARY 3.7. *For every $\varepsilon > 0$, we have*

$$G(n) = O_\varepsilon(n^{1/(3\sqrt{e})+\varepsilon}).$$

Furthermore if $8 \nmid n$, then for all $\varepsilon > 0$,

$$G(n) = O_\varepsilon(n^{1/(4\sqrt{e})+\varepsilon}).$$

Proof. The proof follows directly from Proposition 2.1 and Theorem 3.6.

4. Upper bounds for $w(n)$. The following lemma was proved by H. W. Lenstra, Jr. in [Len] but is proved here using a special case of an inequality for $\psi(x, y)$ due to Konyagin–Pomerance (see [KP]). (The [KP] inequality was also proved by Lenstra in [Len] for the special case needed for the lemma, but only for $p > 3 \cdot 10^9$.)

LEMMA 4.1. *Let p be an odd prime. Then there exists a prime $a < 4 \log^2 p$ with $a^{p-1} \not\equiv 1 \bmod p^2$.*

Proof. Suppose that every prime $a < 4 \log^2 p$ satisfies $a^{p-1} \equiv 1 \bmod p^2$. If b is an integer which can be written as the product of primes less than

or equal to $4\log^2 p$, with $0 < b \leq p^2$, then $b^{p-1} \equiv 1 \bmod p^2$. Recalling the definition of $\psi(x,y)$ from Section 3, the number of such b is at least $\psi(p^2, 4\log^2 p)$. Since $p \geq 3$, we have $p^2 > 4$ and $4\log^2 p > 2$. Theorem 2.1 from [KP] states that for $x \geq 4$, $2 \leq y \leq x$ we have $\psi(x,y) > x^{1-((\log\log x)/\log y)}$. Thus we see that

$$\psi(p^2, 4\log^2 p) > (p^2)^{1-\frac{\log\log(p^2)}{\log(4\log^2 p)}} = (p^2)^{1-1/2} = p.$$

Since p^2 has a primitive root it is easy to see that the number of integers b with $1 \leq b \leq p^2$ and $b^{p-1} \equiv 1 \bmod p^2$ is $p-1$. This is a contradiction to the above result. So there must be some prime $a < 4\log^2 p$ such that $a^{p-1} \not\equiv 1 \bmod p^2$.

It should be remarked that better results than Lemma 4.1 are known. In particular, Granville proved in [Gr] that for prime $p \geq 5$, the least pth power non-residue mod p^2 is less than $\log^2 p$. So there must be some $a < \log^2 p$ with $a^{p-1} \not\equiv 1 \bmod p^2$.

The following lemma is a slight variation of a theorem in [Len].

LEMMA 4.2. *If n is an odd composite number that is not square-free then*

$$w(n) < \log^2 n.$$

P r o o f. Assume that n is odd and that $p^2 \mid n$ for some prime p. Suppose that n is a strong pseudoprime to base a for all positive integers a less than $\log^2 n$. Then for all positive integers a with $a < \log^2 n$, we have $a^{n-1} \equiv 1 \bmod n$, which implies that $a^{n-1} \equiv 1 \bmod p^2$. If we let v be the order of $a \bmod p^2$, by Euler's Theorem we have $v \mid p(p-1)$. Since v also divides $n-1$, we see that $(v,p) = 1$ and thus $v \mid (p-1)$. So for every prime $a < 4\log^2 p \leq \log^2 n$ we must have $a^{p-1} \equiv 1 \bmod p^2$, which is a contradiction to Lemma 4.1. This concludes the proof of this lemma.

COROLLARY 4.3. *For every $\varepsilon > 0$ and each odd composite n,*

$$w(n) = O_\varepsilon(n^{(4\sqrt{e})^{-1}+\varepsilon}).$$

P r o o f. If n is an odd composite that is not square-free then Lemma 4.2 handles this case. Now consider the case where n is an odd composite which is square-free and thus $8 \nmid n$. From Lemma 2.4, we see that $w(n) \leq G(n)$. Applying Corollary 3.7 then gives us our result. This concludes our proof.

As we have seen, Corollary 4.3 follows immediately from our previous results. With more work we will obtain even better upper bounds by considering the number of distinct prime factors of n. Recall the notation ν_2 defined before Lemma 2.2.

LEMMA 4.4. *For every $\varepsilon > 0$, there is some number C_ε with the following property: if p and q are primes that divide an odd number n and $\nu_2(p-1) < \nu_2(q-1)$, then $w(n) \leq C_\varepsilon q^{1/(4\sqrt{e})+\varepsilon}$.*

P r o o f. Taking $\chi(b) = (b/q)$ and $n = q$ in Theorem 3.6 we see that there exists an $a < C_\varepsilon q^{1/(4\sqrt{e})+\varepsilon}$ such that $(a/q) = -1$. So by Lemma 2.3,

$$w(n) \le a < C_\varepsilon q^{1/(4\sqrt{e})+\varepsilon}$$

and we are done.

The earliest form of the following lemma appears to have been given by Vinogradov in 1927 in [V] and later Buchstab (see [Buc]) proved similar results. A good summary of the early literature for first kth power non-residues mod n can be found in Chapter 1 of [N1].

LEMMA 4.5. *For any $\varepsilon > 0$, there exists a constant M_ε such that for every odd prime p and for every $q \in \mathbb{Z}^+$ with $q \mid p-1$ and $q > M_\varepsilon$, there is a qth power non-residue of p less than p^ε.*

We are now ready to prove our first general upper bound result. It should be mentioned that many of the ideas used in the proof of this theorem are from Adleman and Leighton in [AL] where they give a deterministic primality test that runs in time $O_\varepsilon(n^{(1+6\sqrt{e})^{-1}+\varepsilon})$.

THEOREM 4.6. *If n is an odd composite integer and if n is not the product of three distinct primes, then for every $\varepsilon > 0$,*

$$w(n) = O_\varepsilon(n^{1/(8\sqrt{e})+\varepsilon}).$$

P r o o f. By Lemma 4.2, we can assume that n is square-free. We will first prove the result for the case where n has 4 or more distinct prime factors.

Let p, q be the two smallest prime factors of n. Thus we must have $pq \le n^{1/2}$. Two cases will be considered.

(i) $\nu_2(p-1) = \nu_2(q-1)$. Letting $\chi(x) = (x/(pq))$ we see by Theorem 3.6 that there is an $a < C_\varepsilon(pq)^{1/(4\sqrt{e})+\varepsilon}$ such that $(a/(pq)) = -1$. So by Lemma 2.3,

$$w(n) \le a < C_\varepsilon(pq)^{1/(4\sqrt{e})+\varepsilon} = O_\varepsilon(n^{1/(8\sqrt{e})+\varepsilon}).$$

(ii) $\nu_2(p-1) \ne \nu_2(q-1)$. Without loss of generality, we can assume that $\nu_2(q-1) > \nu_2(p-1)$. Then by Lemma 4.4,

$$w(n) < C_\varepsilon q^{1/(4\sqrt{e})+\varepsilon} = O_\varepsilon(n^{1/(12\sqrt{e})+\varepsilon})$$

since $q \le n^{1/3}$.

This concludes the case where there are at least 4 distinct prime factors. Now consider the case where n has exactly 2 distinct prime factors, say p and q, with $p < q$. The proof for this case was suggested by Carl Pomerance. We will consider two cases.

1) $p-1 \nmid q-1$. There must exist a prime r such that $r^b \parallel p-1$ but $r^b \nmid q-1$. Since $n = pq \equiv q \not\equiv 1 \bmod r^b$, $r^b \nmid n-1$. If g is a primitive root mod p and ζ is a primitive rth root of unity, we can define an rth power residue character

$\chi \bmod p$ by setting $\chi(g) = \zeta$. So by Theorem 3.6, we see that there exists an rth power non-residue of p, say a, with $a < C_\varepsilon p^{1/(4\sqrt{e})+\varepsilon} < C_\varepsilon n^{1/(8\sqrt{e})+\varepsilon}$. Now let $v(a)$ be the smallest positive integer with $a \equiv g^{v(a)} \bmod p$. Since a is an rth power non-residue of p, $r \nmid v(a)$. Also

$$1 \equiv a^{l_a(p)} \equiv (g^{v(a)})^{l_a(p)} \bmod p$$

so $p-1 \mid v(a) l_a(p)$ and thus $r^b \mid l_a(p)$. Since $r^b \nmid n-1$, $a^{n-1} \not\equiv 1 \bmod p$ and thus $a^{n-1} \not\equiv 1 \bmod n$. So a is a witness for n and $w(n) \le a = O_\varepsilon(n^{1/(8\sqrt{e})+\varepsilon})$.

2) $p-1 \mid q-1$. First for every $\varepsilon > 0$, let M_ε be the constant from Lemma 4.5 such that for all odd primes p and for all positive integers m with $m \ge M_\varepsilon$ and $m \mid p-1$, there is an mth power non-residue of p less than p^ε. Also let $m = (q-1)/(p-1)$. Once again, two cases will be considered.

(i) $m < M_\varepsilon$. Let r be a prime factor of m and say that $r^b \parallel q-1$. Then $r^b \nmid p-1$. As above there exists an rth power non-residue of q, say a, with $a < C_\varepsilon q^{1/(4\sqrt{e})+\varepsilon}$. As above $r^b \nmid n-1$ but $r^b \mid l_a(q)$ so $a^{n-1} \not\equiv 1 \bmod q$ and thus $a^{n-1} \not\equiv 1 \bmod n$ and a is a witness for n. Since $q < mp = (mn)/q$, we have $q < \sqrt{mn} < \sqrt{M_\varepsilon}\sqrt{n}$. Therefore

$$w(n) \le a < C_\varepsilon(\sqrt{M_\varepsilon n})^{1/(4\sqrt{e})+\varepsilon} = O_\varepsilon(n^{1/(8\sqrt{e})+\varepsilon})$$

and the proof for this case is complete.

(ii) $m \ge M_\varepsilon$. Since $m \mid q-1$, by Lemma 4.5 there is an mth power non-residue mod q, say a, with $a < q^\varepsilon$. So there must be some prime r with $r^b \parallel m$ and $b \ge 1$ such that a is not an r^bth power mod q. Suppose that $r^k \parallel q-1$. Thus, $k \ge b$ and $r^{k-b} \parallel p-1$. Note that

$$n \equiv pq \equiv p \not\equiv 1 \bmod r^{k-b+1}.$$

Let g be a primitive root mod q and as before let $v(a)$ be the smallest positive integer such that $a \equiv g^{v(a)} \bmod q$. Since a is not an r^bth power mod q, we have $r^b \nmid v(a)$ so $\nu_r(v(a), q-1) \le \nu_r(v(a)) \le b-1$. Also we know that $l_a(q) = (q-1)/(v(a), q-1)$. So $\nu_r(l_a(q)) = \nu_r(q-1) - \nu_r((v(a), q-1)) \ge k-b+1$. Since $r^{k-b+1} \nmid n-1$, $a^{n-1} \not\equiv 1 \bmod q$ and so $a^{n-1} \not\equiv 1 \bmod n$. Thus $w(n) \le a \le q^\varepsilon < n^\varepsilon$ and this concludes the proof of Theorem 4.6.

For those n with exactly 3 distinct prime factors we can only prove the following.

THEOREM 4.7. *If n is an odd composite number with exactly 3 distinct prime factors, then for all $\varepsilon > 0$,*

$$w(n) = O_\varepsilon(n^{1/(6\sqrt{e})+\varepsilon}).$$

Proof. From Lemma 4.2 we can assume that $n = pqr$ where p, q, and r are distinct odd primes with $p < r$ and $q < r$. Without loss of generality, two cases can be considered.

(i) $\nu_2(p-1) < \nu_2(q-1)$. By Lemma 4.4, for all $\varepsilon > 0$,

$$w(n) < C_\varepsilon q^{1/(4\sqrt{e})+\varepsilon} = O_\varepsilon(n^{1/(8\sqrt{e})+\varepsilon})$$

with the last step coming from the fact that $q < n^{1/2}$.

(ii) $\nu_2(p-1) = \nu_2(q-1)$. From Theorem 3.6 by letting $\chi(d) = (d/(pq))$ we know that we can find an $a \in \mathbb{Z}^+$ such that

$$a < K_\varepsilon(pq)^{1/(4\sqrt{e})+\varepsilon} \quad \text{and} \quad (a/(pq)) = -1.$$

So from Lemma 2.3 using the fact that $pq \le n^{2/3}$ we must have

$$w(n) \le a < K_\varepsilon(pq)^{1/(4\sqrt{e})+\varepsilon} = O_\varepsilon(n^{1/(6\sqrt{e})+\varepsilon})$$

and this completes the proof of Theorem 4.7.

References

[AL] L. Adleman and F. Leighton, *An $O(n^{1/10.89})$ primality testing algorithm*, Math. Comp. 36 (1981), 261–266.

[AGP] W. R. Alford, A. Granville and C. Pomerance, *On the difficulty of finding reliable witnesses*, in: L. M. Adleman and M. D. Huang (eds.), Algorithmic Number Theory, Lecture Notes in Comput. Sci. 877, Springer, Berlin, 1994, 1–16.

[A] N. Ankeny, *The least quadratic non-residue*, Ann. of Math. 55 (1952), 65–72.

[B1] E. Bach, *Analytic Methods in the Analysis and Design of Number-Theoretic Algorithms*, MIT Press, Cambridge, Mass., 1985.

[B2] —, *Explicit bounds for primality testing and related problems*, Math. Comp. 55 (1990), 355–380.

[BH] E. Bach and L. Huelsbergen, *Statistical evidence for small generating sets*, ibid. 61 (1993), 69–82.

[Buc] A. Buchstab, *On those numbers in an arithmetic progression all prime factors of which are small in order of magnitude*, Dokl. Akad. Nauk SSSR (N.S.) 67 (1949), 5–8 (in Russian).

[Bu1] D. A. Burgess, *On character sums and primitive roots*, Proc. London Math. Soc. 12 (1962), 179–192.

[Bu2] —, *On character sums and L-series II*, ibid. 13 (1963), 524–536.

[Bu3] —, *The character-sum estimate with $r = 3$*, J. London Math. Soc. (2) 33 (1986), 219–226.

[Bur] R. Burthe, *The average witness is* 2, PhD dissertation, University of Georgia, 1995.

[E] P. Erdős, *On pseudoprimes and Carmichael numbers*, Publ. Math. Debrecen 4 (1956), 201–206.

[FT] E. Fouvry and G. Tenenbaum, *Diviseurs de Titchmarsh des entiers sans grand facteur premier*, in: K. Nagasaka and E. Fouvry (eds.), Analytic Number Theory (Tokyo 1988), Lecture Notes in Math. 1434, Springer, Berlin, 1990, 86–102.

[F] V. R. Fridlender, *On the least nth power non-residue*, Dokl. Akad. Nauk SSSR 66 (1949), 351–352 (in Russian).

[Fu] A. Fujii, *A note on character sums*, Proc. Japan. Acad. 49 (1973), 723–726.

[GR] S. Graham and C. J. Ringrose, *Lower bounds for least quadratic non-residues*, in: B. Berndt, H. Diamond, H. Halberstam and A. Hildebrand (eds.), Analytic Number Theory: Proceedings of a Conference in Honor of Paul T. Bateman, Birkhäuser, Boston, 1990, 269–309.

[Gr] A. Granville, *On pairs of coprime integers with no large prime factors*, Exposiotion. Math. 9 (1991), 335–350.

[HW] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 2nd ed., Oxford University Press, London, 1945.

[KS] G. Kolesnik and E. G. Straus, *On the first occurrence of values of a character*, Trans. Amer. Math. Soc. 246 (1978), 385–394.

[KP] S. Konyagin and C. Pomerance, *On primes recognizable in deterministic polynomial time*, in: R. L. Graham and J. Nesetril (eds.), The Mathematics of Paul Erdős, to appear.

[Len] H. W. Lenstra, Jr., *Miller's primality test*, Inform. Process. Lett. 8 (1979), 86–88.

[M] L. Monier, *Evaluation and comparison of two efficient probabilistic primality testing algorithms*, Theoret. Comput. Sci. 12 (1980), 97–108.

[Mo] H. L. Montgomery, *Topics in Multiplicative Number Theory*, Lecture Notes in Math. 227, Springer, New York, 1971.

[N1] K. K. Norton, *Numbers with small prime factors and the least kth power non-residue*, Mem. Amer. Math. Soc. 106 (1971).

[N2] —, *Upper bounds for kth power coset representatives modulo n*, Acta Arith. 15 (1969), 161–179.

[Pa] F. Pappalardi, *On Artin's conjecture for primitive roots*, PhD dissertation, McGill University, 1993.

[P1] C. Pomerance, *On the distribution of pseudoprimes*, Math. Comp. 37 (1981), 587–593.

[P2] —, *Recent developments in primality testing*, Math. Intelligencer 3 (1981), 97–105.

[PSW] C. Pomerance, J. L. Selfridge and S. Wagstaff, Jr., *The pseudoprimes to* $25 \cdot 10^9$, Math. Comp. 35 (1980), 1003–1026.

[R] M. O. Rabin, *Probabilistic algorithm for testing primality*, J. Number Theory 12 (1980), 128–138.

[S] H. Salié, *Über den kleinsten positiven quadratischen Nichtrest nach einer Primzahl*, Math. Nachr. 3 (1949), 7–8.

[Vi] A. I. Vinogradov, *On numbers with small prime divisors*, Dokl. Akad. Nauk SSSR (N.S.) 109 (1956), 683–686 (in Russian).

[V] I. M. Vinogradov, *On the bound of the least non-residue of nth powers*, Bull. Acad. Sci. USSR 20 (1926), 47–58 (= Trans. Amer. Math. Soc. 29 (1927), 218–226.)

10344 Hickory Ridge Road Apt. 418
Columbia, Maryland 21044-4622
U.S.A.
E-mail: rjburth@orion.ncsc.mil

Received on 19.12.1995
and in revised form on 20.5.1996 (2906)